

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-7-LJV-JJM
DECISION & ORDER

The defendant, John Stuart, has been charged in an eight-count indictment with one count of receiving child pornography (18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(b)(1)); four counts of possessing child pornography (18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2)); and one count each of possessing a firearm by a controlled substance user (18 U.S.C. §§ 922(g)(3) and 924(a)(2)), manufacturing marijuana (21 U.S.C. §§ 841(a)(1) and 841(b)(1)(D)), and maintaining a drug-involved premises (21 U.S.C. § 856(a)(1)). Docket Item 8.

Stuart moved to suppress the physical evidence obtained as a result of a search warrant issued by United States Magistrate Judge Michael J. Roemer. Docket Item 27. Likewise, he moved to suppress the statements he later made as fruit of the illegal search. *Id.*

On December 15, 2021, United States Magistrate Judge Jeremiah J. McCarthy issued a Report, Recommendation and Order (“RR&O”) recommending that Stuart’s motion to suppress be denied. Docket Item 33. Stuart objected to the RR&O, Docket Item 36; the government responded, Docket Item 38; and Stuart replied, Docket Item

41. After hearing oral argument, see Docket Item 43, this Court issued a decision and order accepting and adopting Judge McCarthy's RR&O and denying Stuart's motion to suppress. Docket Item 44.

Following this Court's decision and order, Stuart moved to compel discovery, Docket Item 55, and to vacate the protective order, Docket Item 85. He also filed a supplemental motion to suppress evidence and for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978). Docket Item 89. After the government responded to those motions, Docket Items 66, 87, and 92, Judge McCarthy issued a second RR&O ("Second RR&O") denying Stuart's motions to compel and to vacate the protective order and recommending that Stuart's supplemental motion to suppress and for a *Franks* hearing also be denied. Docket Item 99.

On August 7, 2023, Stuart objected to the Second RR&O and appealed Judge McCarthy's denial of his motions to compel and to vacate the protective order. Docket Item 100. On September 27, 2023, the government responded both to the objections and to the appeal. Docket Item 105. This Court then heard oral argument and ordered supplemental briefing on two questions: (1) whether someone's internet protocol ("IP") address is entitled to protection under the Fourth Amendment if that person was actively seeking to keep such information private, and (2) whether information gleaned by virtue of a Fourth Amendment violation can be used to establish probable cause in a subsequent application for a search warrant. See Docket Item 107.

Stuart filed the requested supplemental brief, Docket Item 112; the government responded, Docket Item 116; and Stuart replied, Docket Item 121. This Court then

heard oral argument on the supplemental briefing on January 23, 2024, and reserved decision. See Docket Item 123.

A district court may accept, reject, or modify the findings or recommendations of a magistrate judge. 28 USC § 636(b)(1); Fed. R. Crim. P. 59(b)(3). The court must review *de novo* those portions of a magistrate's recommendations to which a party objects. *Id.*

With respect to non-dispositive motions, however, "a district court may only 'modify or set aside any part of the [magistrate judge's] order that is clearly erroneous or is contrary to law.'" *United States v. Aventura Techs., Inc.*, 607 F. Supp. 3d 278, 282 (E.D.N.Y. 2022) (quoting 28 U.S.C. § 636(b)(1)(A)). "This standard is highly deferential and only permits reversal where the magistrate [judge] abused his discretion." *Id.* (quoting *Mental Disability Law Clinic v. Hogan*, 739 F. Supp. 2d 201, 204 (E.D.N.Y. 2010)).

This Court has carefully and thoroughly reviewed the Second RR&O; the objection, response, and reply; the materials submitted to Judge McCarthy; and the supplemental briefing submitted to this Court. Based on that *de novo* review and for the reasons that follow, this Court accepts in part and modifies in part Judge McCarthy's Second RR&O. More specifically, this Court adopts Judge McCarthy's recommendation to deny Stuart's supplemental motion to suppress and for a *Franks* hearing in its entirety but does so on grounds a bit different than those upon which Judge McCarthy based his recommendation. The Court also finds that Judge McCarthy's denial of the motions to compel and to vacate the protective order was not clearly erroneous or contrary to law and therefore will not disturb that order.

DISCUSSION

This is the second round of pretrial motions challenging the FBI's receipt of information from a foreign law enforcement agency ("FLA") that dismantled several child pornography websites on the Tor network—a computer network designed specifically to facilitate anonymous communication over the internet. The Court assumes the reader's familiarity with the underlying facts and Judge McCarthy's analysis in the Second RR&O, Docket Item 99.

Very briefly, after the FLA uncovered IP addresses that had accessed child pornography websites on the Tor network, it provided those addresses to the appropriate countries to prosecute the individuals who accessed those websites. One such address was linked to Stuart's residence in Cheektowaga, New York, and the FLA transmitted that information to the FBI in Buffalo, New York, in July 2020. After getting authorization to monitor IP activity linked to Stuart's home, the FBI obtained a federal search warrant on October 8, 2020, based on the affidavit of FBI Task Force Officer ("TFO") Michael Hockwater. 20-MJ-5207, Docket Item 2 (search warrant). Following the search, Stuart was charged with the child pornography, narcotics, and firearm offenses noted above.

I. SUPPLEMENTAL MOTION TO SUPPRESS

As already noted, this Court denied Stuart's initial motion to suppress the evidence seized from his home. Docket Item 44. Since then, Stuart says, he has learned that the government's "summary of [its] investigation" in its search warrant application was "intentionally misleading." Docket Item 100 at 4. More specifically, Stuart explains, "[t]he government now claims that one [FLA] seized the server at issue

and another FLA deanonymized the IP addresses provided to them by the first FLA.”

Id. Previously, the government had identified only one FLA. *Id.* at 9-10.

What is more, Stuart asserts, the second FLA “did not disclose to the United States the methodology it used” to obtain Stuart’s IP address. *Id.* at 4. According to Stuart, “[l]acking any transparency in this part of the process, it is impossible to know whether whatever method the second FLA used was a reliable and accurate one.” *Id.* at 5-6. And, he says, “[i]f the government cannot tell this Court how the evidence was gathered, it cannot assure this Court that it does not shock the conscience.” *Id.* at 6-7. In other words, according to Stuart, “[w]ithout this crucial information” about the FLA’s process for obtaining Stuart’s IP address, “the government can make no assurance on the reliability or constitutionality of that process.” *Id.* at 7.

A. Constitutionality

Generally, “[t]he Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country.” *United States v. Getto*, 729 F.3d 221, 227 (2d Cir. 2013) (quoting *United States v. Busic*, 592 F.2d 13, 23 (2d Cir. 1978)). This rule—sometimes referred to as the “international silver platter doctrine”—has two exceptions: (1) “where the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience,” and (2) “where cooperation with foreign law enforcement officials may implicate constitutional restrictions.” *Id.* (quoting *United States v. Lee*, 723 F.3d 134, 140 (2d Cir. 2013)). Here, Stuart suggests that the FLA’s acquisition of his IP address could fall into one or both of these exceptions.

When this Court heard oral argument on Stuart's objection to Judge McCarthy's Second RR&O, it asked the parties a threshold question: whether a person who has been actively seeking to keep his IP address private—for example, by using the Tor network—has Fourth Amendment protections over his IP address. If the Fourth Amendment does not protect an IP address that the user seeks to keep secret, then Stuart's argument is a nonstarter. And after careful review of the parties' submissions and oral argument, this Court finds that there is no Fourth Amendment protection over a person's IP address even when used on the Tor network.

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." *Id.* "A defendant seeking to suppress evidence . . . bears the burden of showing that he had a reasonable expectation of privacy in the place or object searched." *United States v. Sparks*, 287 F. App'x 918, 919 (2d Cir. 2008) (summary order) (citing *California v. Greenwood*, 486 U.S. 35, 39 (1988)).

As Stuart acknowledges, "courts mostly agree that a typical internet user does not have a reasonable expectation of privacy in his or her IP address." Docket Item 112 at 2. "That is because, like phone users who should know that by using their phone they are disclosing information to the phone company, internet users 'should know that [IP] information is provided to and used by Internet service providers for the specific

purpose of directing the routing of information.” *Id.* at 2-3 (quoting *United States v. Ulbricht*, 858 F.3d 71, 96 (2d Cir. 2017)).

The wrinkle here is that Stuart was using the Tor network—a network that is supposed to protect the identity of its users—precisely because he wanted to use the internet covertly. He argues that he therefore had a reasonable expectation of privacy in his IP address. See *id.* at 3-5.

Stuart relies on the Eleventh Circuit’s decision in *United States v. Taylor*, 935 F.3d 1279 (11th Cir. 2019), in which the court observed in a footnote: “That [the defendants] used Tor to download child pornography is important because it takes this case out of third-party-doctrine land.” *Id.* at 1285 n.4 (citing *Smith v. Maryland*, 442 U.S. 735 (1979)). “Instead of traveling along the equivalent of ‘public highways’ (by browsing the open internet) or leaving the equivalent of a calling card at each website visited (as with a normal internet search), Tor users purposefully shroud their browsing, such that they have a reasonable expectation of privacy in their online ‘movements.’” *Id.* (citing *United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015)).

As the government observes, however, whether the defendants had a privacy interest in their IP addresses was not actually litigated in *Taylor*. Docket Item 116 at 6-7. And in a number of other cases where that issue has been litigated, courts have found that there was no Fourth Amendment privacy interest in an IP address used on the Tor network. More specifically, those courts found that even if the individual subjectively expected IP address information to be kept private on a covert network such as Tor (the first prong of the Fourth Amendment privacy-interest test), that is not an expectation that society is willing to recognize as reasonable. See, e.g., *United*

States v. Scanlon, 2017 WL 3974031, *11 (D. Vt. 2017) (finding that “any expectation by a Playpen user [on the Tor network] that his or her identity could not and would not be revealed while accessing child pornography on a publicly available website is not one society would deem reasonable”), *aff’d on other grounds*, 774 Fed. App’x 43 (2d Cir. 2019); *United States v. Matish*, 193 F.Supp.3d 585, 615-17 (E.D. Va. 2016) (holding that a Tor user does not have a reasonable expectation of privacy in his or her IP address); *United States v. Werdene*, 188 F.Supp.3d 431, 445 (E.D. Pa. 2016) (“Even if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not ‘one that society is prepared to recognize as “reasonable.”’” (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967))), *aff’d on other grounds*, 883 F.3d 204 (3d Cir. 2018).

Stuart acknowledges those decisions but urges this Court not to follow them. See Docket Item 112 at 3-4. Among other things, Stuart argues that those cases were decided before the Supreme Court’s decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), which held that there is a right to privacy in cell-site location information (“CSLI”—data generated by a cell phone that can track the user’s location. Stuart analogizes IP address information to the CSLI at issue in *Carpenter*. See Docket Item 112 at 4-5 (“In 2023, using the internet is a requirement of everyday life. Tor users—and anyone who opts for privacy in their internet browsing—understand that their IP address provides an intimate window into the user’s private life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” (quoting *Riley v. California*, 573 U.S. 373, 396 (2014))).

This Court disagrees. After careful consideration, this Court finds that even if Stuart subjectively expected that he was keeping his IP address private by using Tor, that expectation of privacy is not one that society is willing to recognize as reasonable.

First, as several courts have noted, a Tor user still gives his information to the “entry node” on the system. See *Matish*, 193 F.Supp.3d at 616-617 (explaining that “in order for . . . prospective user[s] to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations” (quoting *United States v. Farrell*, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016))); *Werdene*, 188 F. Supp. 3d at 444 (finding that the defendant “had no reasonable expectation of privacy in his IP address” because “[a]side from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user’s IP address to a third-party”). “Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers.” *Farrell*, 2016 WL 705197, at *2.

What is more, “the Tor Project itself even warns visitors ‘that the Tor network has vulnerabilities and that users might not remain anonymous.’” *Matish*, 193 F. Supp. 3d at 616 (quoting *Farrell*, 2016 WL 705197, at *2); see also 20-MJ-5207, Docket Item 1 at ¶ 12 (Hockwater affidavit) (explaining that “[t]he Tor Project maintains a publicly available frequently asked questions (FAQ) page,” which includes “the question ‘So I’m totally anonymous if I use Tor?’ . . . , to which the response is, in bold text, ‘No.’”) Thus, as a number of other courts have found, any “subjective expectation of privacy . . . is not objectively reasonable.” *Matish*, 193 F. Supp. 3d at 616.

Moreover, the Court is troubled by the notion that a defendant could “serendipitously receive Fourth Amendment protection’ because he used Tor in an effort to evade detection, even though an individual who does not conceal his IP address does not receive those same constitutional safeguards.” *Werdene*, 188 F. Supp. 3d at 446 (quoting *United States v. Stanley*, 753 F.3d 114, 121 (3d Cir. 2014)). That, too, does not strike this Court as reasonable, and the Court believes that the expectation of privacy at issue is not one that society is willing to recognize as reasonable.

Nor is this Court persuaded by Stuart’s analogy to *Carpenter*. On the contrary, courts “consider[ing] the application of *Carpenter* in this context ha[ve] declined to extend its reasoning to IP address information.” *United States v. Kidd*, 394 F. Supp. 3d 357, 362 (S.D.N.Y. 2019).

For example, in *United States v. Morel*, 922 F.3d 1 (1st Cir. 2019), the First Circuit rejected the defendant’s argument that *Carpenter* “ha[d] effected a sea change in the law of reasonable expectation of privacy” such that he now had a Fourth Amendment privacy interest in his IP address. *Id.* at 8. Among other things, the court explained that “unlike CSLI, ‘an internet user generates the IP address data . . . only by making the affirmative decision to access a website or application.’” *Id.* (alteration in original) (quoting *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019)). “By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger.” *Hood*, 920 F.3d at 92.

Although the Second Circuit has not yet weighed in on this precise issue, district courts in this circuit have held that *Carpenter* did not disturb the case law holding that there generally is no reasonable expectation of privacy in an IP address. See *United States v. Hernandez*, 2020 WL 3257937, at *21 (S.D.N.Y. June 16, 2020); *Kidd*, 394 F. Supp. 3d at 362; *United States v. Germain*, 2019 WL 1970779, at *4 (D. Vt. May 3, 2019).¹ This Court agrees. And the fact that Stuart used Tor to attempt to conceal his IP address does not change the calculus for the reasons explained above.

Thus, this Court finds that Stuart did not have a reasonable expectation of privacy in his IP address.² As a result, the FLA's obtaining of his IP address was not a search and is therefore not subject to the Fourth Amendment's exclusionary rule.³

¹ The acquisition of cell phone information that "provides geographically accurate information that follows a defendant's day-to-day movements" is not as clear-cut as using an IP address to search the Internet and "requires a precise understanding of the technology at issue." *Kidd*, 394 F. Supp. 3d at 367-68 (finding that the defendant had "not met his burden of showing that he ha[d] a reasonable expectation of privacy in the IP address information collected by [a telecommunications provider] and subpoenaed by the [g]overnment, because there [wa]s an insufficient record to support a conclusion that such information reflected the whole of [the defendant's] locations and movements"). But that type of information is not at issue in this case.

² Judge McCarthy reached this same conclusion in the context of Stuart's motion to compel. See Docket Item 99 at 9 (explaining that Stuart has not "established a reasonable expectation of privacy in the content of the Target Website's host server").

³ The second FLA represented to the United States government that "at no time was any computer or device interfered with in the United States" and that the FLA "did not access, search[,] or seize any data from any computer in the United States." Docket Item 75-1 at 12. Stuart attempts to cast doubt on that assertion. See Docket Item 89 at 11-12. But as Judge McCarthy noted, even if the FLA used malware technology such as a Network Investigation Technique (NIT)—notwithstanding its representation to the United States government to the contrary—"there is nothing to suggest that TFO Hockwater was aware of this." Docket Item 99 at 20. Thus, to extent that the FLA did conduct a search to obtain Stuart's IP address, then the good faith exception would apply for the reasons Judge McCarthy articulated. See Docket Item 99 at 22-23.

B. Reliability

With respect to reliability, this Court agrees with Judge McCarthy that “none of [Stuart’s] additional arguments or information undermine the indicia of reliability that [this Court] previously concluded existed from the information presented in the four corners of TFO Hockwater’s [a]ffidavit.” Docket Item 99 at 22. In particular, none of the new information casts doubt on the assertion in Hockwater’s affidavit that the second FLA—which obtained Stuart’s IP address and relayed that information to the FBI—had a “track record of sharing and providing reliable and accurate information” to the United States. See Docket Item 44 at 8. That assertion, as this Court stated in its prior decision and order, “was and is critical to determining reliability.” *Id.*

Alternatively, the good faith exception applies for the reasons stated by Judge McCarthy in the Second RR&O and by this Court in its prior decision and order. See *id.* at 11-12; Docket Item 99 at 22-23.

II. MOTION FOR A *FRANKS* HEARING

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing if he makes “a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause.” 438 U.S. at 155-56. Mere conjecture is not enough, however; instead, to be entitled to a *Franks* hearing, a defendant must make “a substantial preliminary showing” of a “false statement [that] is necessary to the finding of probable cause.” *Id.*

As Judge McCarthy observed, “[t]he primary source of probable cause for the search warrant for Stuart’s residence was [the second FLA’s] tip that ‘on May 28, 2019, [an IP address later determined to be associated with Stuart] “was used to access online child sexual abuse and exploitation material” via . . . the [Target Website].’” Docket Item 99 at 20 (quoting 22-MJ-5207, Docket Item 1 at ¶ 24). This Court agrees with Judge McCarthy that Stuart has not made the required “substantial preliminary showing” of an intentional or reckless false statement with respect to that assertion. See *id.* at 16-20.

At oral argument, Stuart’s counsel suggested that even if this Court were to find that Stuart does not have a privacy interest in his IP address, it still should order a *Franks* hearing to determine whether there was some further invasion of privacy—such as obtaining content from Stuart’s home computer. This Court declines that invitation.

As explained above, see *supra* note 3, this Court agrees with Judge McCarthy that—even assuming for the sake of argument that the FLA conducted a search of Stuart’s computer despite its assertion to the contrary—“there is nothing to suggest that TFO Hockwater was aware of this.” See Docket Item 99 at 20. Thus, Stuart has not met the “high” burden required for a *Franks* hearing. See *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991).

III. MOTION TO COMPEL AND MOTION TO VACATE THE PROTECTIVE ORDER

As explained above, this Court cannot set aside Judge McCarthy’s decisions on Stuart’s motions to compel and to vacate the protective order unless they were clearly erroneous or contrary to law. This Court agrees with the government that Stuart has not identified any defects in Judge McCarthy’s orders that meet this high bar. See Docket Item 105 at 23-25. Accordingly, those orders are affirmed.

CONCLUSION

For the reasons stated above, this Court adopts Judge McCarthy's recommendation, Docket Item 99, to deny Stuart's supplemental motion to suppress and for a *Franks* hearing. Stuart's supplemental motion to suppress and for a *Franks* hearing, Docket Item 89, is DENIED. Judge McCarthy's decisions on Stuart's motion to compel, Docket Item 55, and motion to vacate the protective order, Docket Item 85, are AFFIRMED.

SO ORDERED.

Dated: February 22, 2024
Buffalo, New York

/s/ Lawrence J. Vilardo

LAWRENCE J. VILARDO
UNITED STATES DISTRICT JUDGE